UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/807,615	07/13/2001	Christophe Clavier	032326133	2076

21839 7590 06/30/2005

BUCHANAN INGERSOLL PC
(INCLUDING BURNS, DOANE, SWECKER & MATHIS)
POST OFFICE BOX 1404
ALEXANDRIA, VA 22313-1404

EXAMINER	
ZIA, SYED	
ART UNIT	**PAPER NUMBER**
2131	

DATE MAILED: 06/30/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/807,615	CLAVIER ET AL.	
	Examiner	Art Unit	
	Syed Zia	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *13 July 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-8 and 11-15* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-8, and 11-15* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *07/13/2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date 4/16/2001
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

This office action is in response to application filed on July 13, 2001. Original application contained Claims 1-15. Applicant submitted preliminary amendment to cancel claims 9-10, amended Claims 1-8, and added new claims 11-15. Therefore, Claims 1-8, and 11-15 are pending for consideration.

Claim Rejections - 35 USC § 102

> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

1. Claim 11-15 are rejected under 35 U.S.C. 102(e) as being anticipated by Kocher et al. (U. S. Patent 6,278,783).

2. Regarding Claim 11 Kocher teaches an electronic security component have a countermeasure against attacks on a secret key cryptography technique in which data is manipulated by critical instructions (Firg.1-2, abstract), said component comprising:

a program memory having stored therein a plurality of manipulating means for use during said critical instructions, said manipulating means having complementary input and/or output data relative to one another (col.2 line 25 to line 36); and

means for generating a random value that designates at least one of said manipulating means to be employed during a given execution of said cryptography technique (col.6 line 39 to line 67).

3. Claims 12-15 are rejected applied as above rejecting Claim 11. Furthermore, Kocher teach and describe an electronic security component, wherein

As per Claim 12 said plurality of manipulating means each comprise a table of constants (col.7 line 15 to line 65).

As per Claim 13 said cryptography technique comprises a DES algorithm that is executed in multiple rounds (col.9 line 1 to col.10 line 39, and col.11 line 41 to line 55).

As per Claim 14 said random value has a first state which designates a manipulating means that is to be employed during all of the rounds of said algorithm, and a second state which designates at least two other manipulating means that are to be employed during different respective rounds of said algorithm (col. 2 line 25 to col.3 line 9).

As per Claim 15 said component is a chip card (col.14 line 1 to line 8).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 1-8 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kocher (U. S. Patent 6,278,783) and further in view of Leppek et al (U. S. Patent 5,933,501).

5. Regarding Claim 1 Kocher teaches a countermeasure method in an electronic component using a secret key cryptographic algorithm for calculating an encoded message from an input message of the type in which sixteen calculation rounds are employed where each round supplies an output data item from an input data item (col.6 line 39 to line 42, and col.9 line 1 to col.10 line 38), and the output data item is manipulated by critical instructions in at least the first three and last three rounds (col.9 line 14 to line 67), said method including the following steps:

forming a group comprising at least the first three rounds and another group comprising at least the last three rounds (col.9 line 14 to line 17)),

selecting the sequence to be executed in the groups as a function of a statistical half probability distribution in order to make the data manipulated by said critical instructions unpredictable (col.5 line 8 to line 15, col.6 line 29 to line 63,and col.9 line 5 to line 23).

Although the system disclosed by Kocher shows all the features of the claimed limitation, but Kocher does not specifically disclose applying a first sequence that uses a first manipulating means for said critical instructions in each round or a second sequence that uses other manipulating means for said critical instructions at least in certain rounds and statistical probability distribution

In an analogous art, Leppek, on the other hand discloses a data communication control mechanism to securely encrypt data communication that effectively prevents a usurper form from decrypting the (abstract) wherein: applying a first sequence that uses a first manipulating means for said critical instructions in each round or a second sequence that uses other manipulating means for said critical instructions at least in certain rounds, said first and second sequences being such that they supply the same result at the output from the last round in each group for the same given input message (Fig.2, col.4 line 7 to line 51), and

selecting the sequence to be executed in the groups as a function of a statistical half probability distribution (col.4 line 33 to line 53),

Therefore, It would have been obvious to one ordinary skilled in the art at the time of invention to combine the teachings of Kocher and Leppek, because Leppek's method of executing other manipulating means, such as derived from first manipulating means for critical instruction to deliver output data on the basis of input data by using algorithm of series of encryption operator with randomized order to obscure the encryption footprint will not only make Kocher's cryptosystem data more unpredictable and prevent attacks.

6. Claims 2-8 are rejected applied as above in rejecting Claim 1. Furthermore, the system of Kocher, and Leppek teaches and describes a system and method of countermeasure, wherein:

As per claim 2, each of said manipulating means produces output data in accordance with input data, and wherein said other manipulating means are such that they complement at least one or both of the input and/or output data of the first manipulating means.

As per Claim 3 said second sequence comprises, for one or more rounds, an additional complementation operation at the input or output of the manipulating means used, and wherein said first sequence includes an additional operation of identical copying that corresponds to each additional complementation operation in said second sequence (Kocher: col. 6 line 29 to line 63, and col.9 line 5 to line 23, Leppek: col.4 line 10 to line 23).

As per claim 4 four groups of each of four successive rounds are formed, and wherein said first sequence is applied to each group and said second sequence is applied to at least the first group and the last group (Kocher: Fig.1 col.9 line 1 to col.10 line 38).

As per Claim 5 second sequence is applied to each of the groups Kocher: col. 6 line 29 to line 63, and col.9 line 5 to line 23, Leppek: col.4 line 10 to line 23).

As per Claim 6 the first group is formed by the first three rounds and the last group is formed by the last three rounds (Leppek: col.4 line 10 to line 23).

As per Claim 7, the step of selecting the sequence to be executed is made at the start of execution of the algorithm by drawing a random value (Kocher: col.6 line 39 to line 53).

As per Claim 8 said manipulating means are tables of constants (col. 7 line 16 to line 65).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Syed Zia whose telephone number is 571-272-3798. The examiner can normally be reached on 9:00 to 5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

sz
June 18, 2005